



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



020.205 IT System Technical Assessments Policy

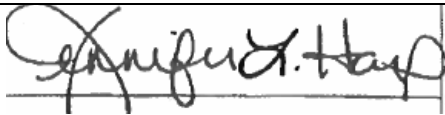

**Version 2.2
November 15, 2018**

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

Revision History

Date	Version	Description	Author
5/2/2005	1.0	Effective Date	CHFS IT Policies Team Charter
11/15/2018	2.2	Review Date	CHFS OATS Policy Charter Team
11/15/2018	2.2	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	11/15/2018	Jennifer Harp	
CHFS Chief Information Security Officer (or designee)	11/15/2018	DENNIS E. LEBER	

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE	6
3	ROLES AND RESPONSIBILITIES	6
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	6
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
4	POLICY REQUIREMENTS	7
4.1	GENERAL	7
4.2	SECURITY IT STAFF RESPONSIBILITY	8
4.3	ASSESSMENTS DETAILS	8
5	POLICY MAINTENANCE RESPONSIBILITY	8
6	POLICY EXCEPTIONS	9
7	POLICY REVIEW CYCLE.....	9
8	POLICY REFERENCES	9

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

1 Policy Definitions

- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Critical Systems:** Any system or application that is federally mandated/regulated, deemed critical by the data or system owner(s), or deemed a “24 hours, 7 days a week, 365 days a year” (24x7x365) application, will be defined as a critical system. CHFS ITMP will be the source of knowledge and repository of severity level for systems/applications.
- **Discovery:** Manually walking through the web application to understand the logic and operational flows in order to filter out information that may generate messages or email triggered by scanning.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual’s tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person’s tax liability or potential tax liability.
- **Manual Penetration Test:** Examine specific flaw categories that currently require manual inspection to evaluate the security of the infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations, or risky end-user behavior.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual’s identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual’s personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother’s maiden name, etc.).
- **Security Review:** The security assessment will end with a list of all vulnerabilities that are found through the web. Risk should be prioritized based on the ease of exploiting the vulnerability and the potential harm that could result if an attacker is successful. The results will be disseminated to the project team, who will then prioritize what needs to be fixed so that existing applications can be hardened. Those applications being built can be remedied and safely placed into production.

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.
- **Vulnerability Assessment:** Results from the automated scanning process, delivering a report that details non-verified issues that will require further research and validation.
- **Vulnerability Scan:** The execution of automated security scanning software that attempts to discover, define, identify, and classify the lapse in security in a web application or network system. This automated vulnerability scan is considered intrusive.

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through a system technical assessment policy. This document establishes the agency's Information Technology (IT) System Technical Assessments to manage risks and provide guidelines for security best practices regarding the agency's IT assessments.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 General

CHFS complies with and adheres to the Commonwealth Office of Technology (COT) [Enterprise CIO-082 Critical Systems Vulnerability Assessments Policy](#). CHFS OATS works collaboratively with program areas to determine the level of sensitivity for its data.

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

The CHFS executive leadership along with business partners and other stakeholders shall define the agency's critical systems that are subject to meet the assessments listed and defined within this policy. Although not mandatory, all other agency systems containing sensitive data, but not deemed critical, should also comply with IT Technical assessment requirements outlined in this policy.

CHFS utilizes the NIST federal standards as well as FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems for determining its critical systems. Utilizing FIPS 199, a system is defined as critical when the potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Per Enterprise CIO-082 Policy, for those systems deemed critical, the CHFS is responsible for engaging a third party to assist in conducting vulnerability assessments both upon implementation into production and every two (2) years thereafter.

CHFS also follows [065.014 CHFS Software Development Lifecycle \(SDLC\) and New Application Development Policy](#) and [CHFS 040.201 Internal Risk Assessment Policy](#). Vulnerability assessments can be performed by the internal CHFS OATS IS Team or contracted to an approved third party vendor.

4.2 Security IT Staff Responsibility

CHFS OATS IS Team is responsible for oversight of vulnerability assessments of each system covered by this policy. If the agency decides to use a third party vendor, the CHFS IS Team is responsible to ensure the third party vendor is qualified and approved by CHFS management. The CHFS OATS IS Team will maintain a list of internal and third party assessments performed within OATS. This list will identify the assessment performed, application assessed, date(s) of the assessment or retesting, and the party performing the assessment. The CHFS OATS IS Team is responsible for updating this policy, as well as associated procedures when changes to the infrastructure or enterprise environment occur.

4.3 Assessments Details

CHFS OATS IS Team utilizes a layered approach methodology to application security testing. The methodology for this assessment includes Discovery, Vulnerability Scanning, Manual Penetration Testing, Vulnerability Assessments, and Security Reviews.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

020.205 IT System Technical Assessments Policy	Current Version: 2.2
020.200 Managerial Security	Review Date: 11/15/2018

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 040.201 Internal Risk Assessment Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Risk Assessment Program Procedure
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information